A propos du projet de loi dit n° 214. La lutte de la criminalité dans le cyberespace à l'épreuve au principe de régularité des preuves

Poullet, Yves

Published in:
Liber Amicorum J. du Jardin

Publication date:
2001

A propos du projet de loi dit n° 214[1]

La lutte de la criminalité dans le cyberespace à l'épreuve du principe de régularité des preuves[2]

Yves Poullet[3]

Doyen de la Faculté de Droit de Namur
Professeur à la Faculté de Droit de Liège
Directeur du CRID
yves.poullet@fundp.ac.be
http://www.droit.fundp.ac.be/crid.htm

[1] Projet de loi relatif à la criminalité informatique, *Doc. Ch. Repr.,* 0213/008, 14 juillet 2000, Sess. 1999-2000 disponible sur le site de la Chambre : http://www.lachambre.be. Ce projet de loi a été approuvé par la Chambre des Représentants en première lecture, amendé par le Sénat (*Doc. Sénat* 2-392, Sess. 1999-2000) et est actuellement en seconde lecture à la Chambre. Il résulte de la fusion de deux projets dont l'origine remonte au gouvernement précédent. Il s'agit du projet de loi n° 213 relatif à la criminalité informatique qui définit de nouveaux délits qui constituent une infraction contre la confidentialité, l'intégrité et la disponibilité des systèmes informatiques ou des données qui sont stockées, traitées ou transmises par le biais de ces systèmes et du projet de loi n° 214 qui, sous le même titre, a pour objet les nouvelles techniques de dépistage comme la confiscation des données, l'obligation de coopération des opérateurs de services de télécommunications, la recherche de réseau et l'interception des communications.

[2] La rédaction de l'article s'inscrit dans le cadre du projet PAI n° 31 « Société de l'Information » (Pôle d'Attraction Universitaire) financé par les SSTC (Services du Premier Ministre). L'auteur remercie chaleureusement Florence de Villenfagne pour sa relecture et ses suggestions lors de la rédaction du texte.

[3] L'auteur s'exprime à titre personnel et n'entend en aucune manière représenter les vues de la Commission de la Protection de la Vie Privée dont il est membre.

« Sous le régime de l'administration libre de la preuve en matière pénale, les éléments probants ne peuvent pas être recueillis d'une manière illégale. …

Il est à l'évidence, interdit aux organes du pouvoir d'agir, non seulement en violation d'un texte formel de la loi mais aussi d'une manière irrégulière, c'est-à-dire en violant les principes généraux du droit, … »
(J. du Jardin)[4].

1. Ces conclusions de notre collègue et ami Jean du Jardin, par ailleurs reprises et amplifiées par l'arrêt de la Cour[5] et depuis par une doctrine et jurisprudence abondantes[6] mettaient fin à une controverse doctrinale et jurisprudentielle, entre les tenants de la preuve libre et celle de la preuve réglementée[7]. Elles affirmaient haut et fort que la liberté de preuve que le Code d'Instruction criminelle consacre[8], ne peut signifier le droit du juge ou des autorités en charge de l'établissement des infractions de recourir à tout procédé pour ce faire. « Car s'il n'y a pas de régime légal des preuves, il y a un régime de la recherche ou de l'administration des preuves »[9].

2. Ce régime obéit aux règles légales qui, le cas échéant, entourent le mode de production ou d'établissement d'une infraction mais, au-delà de ces règles, à des principes généraux du droit comme celui du droit au silence de l'inculpé, du respect de la vie privée, etc. C'est dans la mesure où la Justice et la loi veilleront au respect de cette double exigence que sera garanti, selon le propos de Mr. Montanari[10], un « Etat de droit » et rejeté un « Etat absolu » : « Dans le premier, la garantie de la liberté est résiduelle puisqu'elle est subordonnée à l'intérêt public de la constatation de la vérité ; le citoyen « soumis » même devrait être intéressé avant tout à la réalisation du bien public. Dans le second, le cadre de la défense de la liberté est tout à fait différent ; il dépend de la raison philosophique, pour laquelle le droit garantit la liberté comme condition constituant chaque homme, avant même qu'il soit citoyen ».

3. Le projet de loi sur la criminalité informatique que le Sénat vient de renvoyer amendé à la Chambre des représentants suivant la procédure bicamérale incomplète[11], contient dans sa seconde partie des dispositions

---

[4] Il s'agit des conclusions que J. du JARDIN, alors avocat général, avait prononcées dans une affaire fiscale en cause Vande Vyvere et consorts, soumis à la Cour de Cassation (Cass. 13 mai 1986, *Pas*., 1987, p. 1107).

[5] « Est illégale la preuve obtenue par un acte qui est expressément interdit par la loi, mais aussi par un acte qui est inconciliable avec les règles substantielles de la procédure pénale ou avec les principes généraux du droit » (arrêt précité, p. 1110).

[6] A ce propos, not. R. DECLERCQ, « La preuve en matière pénale »Bruxelles, Swinnen, 1988, p. 43 et s. et P. MANDOUX, « Aspects récents de la légilatié de la preuve en droit pénal », Droit pénal des affaires, Bruxelles, éd. Jeune Barreau, 1991, pp. 34 à 37.

[7] Cf. déjà sur cette controverse not. , A. MASSET, « Limites de certains modes de preuve » *in Les droits de la défense en matière pénale*, Actes du colloque des 30-31 mai et 1er juin 1985, Barreau de Liège, Ed. Jeune Barreau de Liège, 1985, p. 161 ; P.E. TROUSSE, « La preuve des infractions », *R.D.P*., 1958-59, p. 742 ; R. LEGROS, « La preuve légale en droit pénal », *J.T*., 1978 , p. 598 et s. ; J. MESSINE, « La vie privée et le droit de la preuve en matière pénale », *Ann. Dr. de Louvain*, 1984, p. 403 et s.

[8] Cf. à cet égard, le fait que la jurisprudence (Cass. 17 août 1978, *Pas*., 1978, I, 1259 ; Cass. sept. 1972, *Pas*. 1973, I, 11) et la doctrine ont toujours considéré que la liste des moyens de preuve à laquelle l'article 154 du Code d'Instruction criminelle se réfère est purement énonciative et n'interdit pas au juge d'accepter d'autres moyens de preuve que ceux prévus par la loi (A cet égard, not. J. MESSINE, *op.cit.,* pp. 406 et 407).

[9] Selon la formule célèbre du pénaliste français Jean PRADEL, *Procédure pénale*, Paris, 5e éd., n° 258.

[10] B. MONTANARI, « La « faute » et « l'accusation » : réflexions sur la Vérité dans le procès », *Int. Rev. of Penal Law*, 19, p. 43 et s. L'auteur souligne qu'une procédure inquisitoire constitue volontiers une manifestation de la supériorité de l'Etat et, dès lors, pourrait conduire facilement à un Etat absolu si des limites à la production des preuves ne sont pas mises. L'auteur ajoute, à propos de l'adoption de cette procédure, la justification suivante : « En effet, puisque le procès inquisitoire, à cause de sa justification rationnelle, est une manifestation de la puissance de l'Etat, dans son unicité et souveraineté, et puisque, même du point de vue de la symbologie et de l'imaginaire collectifs, il défend la collectivité plutôt que l'individu dans sa liberté, il paraît donc, plus apte à tenir tête à des situations de grande désagrégation idéale et sociale et à des phénomènes de criminalité organisée qui portent atteinte à l'intégrité de la personne ».

[11] L'exigence de mettre en œuvre la procédure bicamérale complète visée à l'article 77 de la Constitution et non la procédure incomplète de l'article 78 était réclamée par le Conseil d'Etat. Elle s'explique par la modification que propose la loi aux compétences du juge d'instruction

modifiant ou complétant le Code d'instruction criminelle. Ces dispositions entendent légaliser de nouveaux modes d'investigation et de recherche d'infractions en tenant compte du fait que celles-ci se réalisent par des moyens utilisant les technologies de l'information et de la communication ou laissent des traces dans de tels systèmes.

Le projet s'inspire des travaux actuellement réalisés dans des enceintes internationales[12], en particulier de la recommandation n° R (95) 13 du Conseil de l'Europe[13].

4. Notre propos est, commentant les dispositions du projet belge, de les analyser à l'aune du principe de la régularité des preuves. Certes, s'il est indispensable au regard des risques nouveaux créés par l'utilisation des systèmes d'information et des réseaux de permettre la lutte efficace des autorités publiques en facilitant la détection, l'investigation et la poursuite des infractions, il est, dans la même mesure, nécessaire de garantir l'équilibre entre les intérêts de cette action répressive et le respect des droits fondamentaux des citoyens[14], en particulier leur vie privée.

Cet équilibre peut être facilement rompu. En effet, souvent les autorités publiques ont dénoncé l'opacité des systèmes d'information, la fugacité de l'information qui y circule voire sa non transparence ; cependant l'utilisation de ces mêmes systèmes par les citoyens laisse des traces qui permettront sans doute avec le concours d'opérateurs privés, mieux que dans le contexte traditionnel, de contrôler et de cerner les dires, faits et déplacements de chacun et ce aux risques d'une société dite de surveillance.

(cf. avis du Conseil d'Etat, *Doc. Parl*., 213/001, p. 56). Le gouvernement et le Parlement n'ont pas fait suite à cette observation du Conseil d'Etat.

[12] Outre le Conseil de l'Europe, cf. les travaux de l'Union européenne, de l'OCDE et du G8 (à cet égard, E. WERY, « Le Conseil de l'Europe et le G.8 se penchent sur la criminalité informatique », *Actualité*, Mai 2000, disponible sur le site Droit et Nouvelles Technologies http://www.droit-technologies.org.

[13] Recommandation n° R(95)13 du Comité des Ministres aux Etats membres relative aux problèmes de procédure pénale liés à la technologie de l'Information (adoptée le 11 sept. 1995) disponible sur le site du Conseil de l'Europe : http://www.coe.fr/cm/ta/rec/1995/f95r13.htm. Le Conseil de l'Europe discute à l'heure actuelle d'un « Projet de convention sur la cyber-criminalité (projet dit n° 19). Ce projet est actuellement soumis à débat public. Il est disponible sur le site du Conseil de l'Europe http://www.conventions .coe.int/treaty/fr/projets/cybercrime.htm.

[14] …comme le concluait H. BOSLY, « La régularité de la preuve en matière pénale », *JT*, 1992, p. 128.

SECTION 1 : LE CONTEXTE :
QUI A PEUR DE QUOI ? ET POURQUOI ?

5. L'OCDE définit la criminalité informatique comme « tout comportement illégal ou contraire à l'éthique ou non autorisé qui concerne un traitement automatique de données et/ou une transmission de données »[15].

Selon Ph. Rose[16] qui note l'évolution et l'adaptation du crime informatique aux réalités sociales mais surtout aux technologiques nouvelles, au début des années 80, époque de la banalisation des ordinateurs en entreprises, une première vague de criminalité touche essentiellement le piratage de logiciels vu leur coût et la faible offre sur le marché. Mais la menace était essentiellement interne aux entreprises. A la fin des années 1980 par contre, l'émergence des réseaux, et depuis 1993 celle des réseaux « globaux » que constitue notamment la toile d'Internet, justifie que la menace soit devenue externe avec des phénomènes tels le « hacking », le « phreaking », le « cracking », le blocage des sites, etc. Ainsi, l'ordinateur, ou plus largement un système d'information, peut être la cible, l'instrument ou l'objet même d'un crime.

6. A ces diverses facettes du phénomène de la criminalité informatique correspond une liste de nouvelles infractions dont le Conseil de l'Europe[17] tente d'unifier les définitions et dont certaines sont introduites en droit belge par le projet de loi dit 213 sur la criminalité informatique[18].

Les récentes attaques contre les célèbres sites commerciaux américains (ebay et Amazon), le virus « I love You », la multiplication des copiages illicites de logiciels permettant de lire ou d'écrire des morceaux de musique en format MP3 « attirent l'attention de l'opinion internationale sur les dangers auxquels Internet et

---

[15] OCDE, *La fraude liée à l'informatique : analyse des politiques juridiques*, Paris, 1986, p. 7 ; Pour d'autres définitions et leur analyse, lire R. KASPERSEN, *Strafbaarstelling van computermisbruik*, Kluwer, 1990, p. 29 et s. Sur le phénomène et son ampleur, le lecteur consultera notamment P. GALLEY, « Terrorisme informatique : quels sont les risques ? » disponible sur http://home.worldcom.ch/pgalley/inforce/sts/crime-html ; U. SIEBER, « Legal Aspects of Computer-related crime » *in The Information Society-COMCRIME Study-Rapport pour la Commission européenne*, 1998 ; P. Van EECKE, *Criminaliteit in cyberspace*, Mijs & Breesch, 1997 ; D. MARTIN, *La criminalité informatique*, PUF, 1997 ; …

[16] Ph. ROSE, « Délinquance informatique, Inforoutes et nouvelle guerre de l'information », *Les cahiers de la sécurité intérieure*, Paris, La Documentation française, n° 24, 1996.

[17] Il s'agit de la Recommandation n° (89)9 du Comité des Ministres du Conseil de l'Europe sur la criminalité en relation avec l'ordinateur. Cette Recommandation incite les Etats-membres à insérer dans leur dispositif juridique des sanctions adéquates en ce qui concerne certaines agissements à l'égard des systèmes informatiques, des données ou des programmes d'ordinateur. En annexe de cette recommandation figure une liste reprenant les types d'agissements pour lesquels les Etats devraient intervenir (liste dite minimale), ainsi que ceux pour lesquels l'intervention législative est laissée au libre choix des Etats (liste facultative). Cette liste comporte les activités criminelles suivantes :

Liste minimale

1. Fraude informatique
2. Faux en informatique
3. Dommages affectant les données et les programmes
4. Sabotage informatique
5. Accès non autorisé à des systèmes informatiques
6. Interception non autorisée
7. Reproduction non autorisée de programmes d'ordinateur ou de topographies

Liste facultative

8. Altérations de données ou de programmes d'ordinateur
9. Utilisation non autorisée d'un ordinateur
10. Utilisation non autorisée d'un programme

[18] Le projet de loi dit 213 introduit les infractions suivantes : le faux en informatique, la fraude informatique et les infractions contre la confidentialité, l'intégrité et la disponibilité des systèmes informatiques et des données.
Sur ces diverses infractions, lire le remarquable rapport d'Ulrich SIEBER, « Legal Aspects of Computer-related crime in the Information Society-COMCRIME Study, LAB, DG XIII, E.U., 1998 ;

d'autres réseaux informatiques doivent faire face : les cybercriminels et les cyberterroristes menacent les intérêts des entreprises et des gouvernements et peuvent provoquer des dégâts considérables »[19]. Ces craintes justifient non seulement la définition de nouvelles infractions, mais surtout de nouveaux modes de travail et d'enquête des autorités chargées de la répression de ces infractions au plan national, mais également et surtout international[20].

7. L'omniprésence des technologies de l'information et de la communication dans la vie des entreprises et des citoyens oblige les autorités policières et judiciaires à une radicale adaptation de leurs méthodes d'investigations et d'instruction criminelle. Au moment où l'ordinateur a remplacé les armoires de classement et où les réseaux partagent, le cas échéant aux 4 coins du monde, les conversations, les fichiers, les images, etc., ces nouvelles procédures : - le droit de perquisitionner les systèmes d'information, de conserver ou faire conserver les données « saisies », la possibilité d'intercepter les données transmises par les réseaux, de la décoder, la collaboration avec les opérateurs de télécommunication et les fournisseurs de services informatiques (d'hébergement, de cryptage, d'archivage, d'accès à Internet) - sont indispensables pour poursuivre pratiquement n'importe quelle infraction dans la mesure où le système d'information le réseau, gardera et révélera la trace d'un projet d'attentat terroriste[21], de l'escroquerie d'un comptable, de la diffusion ou possession d'images pédophiles ou de propos racistes, etc.

8.. Quelques caractéristiques des systèmes d'information, qui expliquent et justifient les modifications et ajouts introduits par le projet de loi 214 dans le code d'Instruction criminelle belge, méritent d'être soulignées. Elles.

Une **première caractéristique** est certes l'immatérialité des « documents » qui ne s'attachent pas à un support matériel précis, mais dont le contenu peut facilement être déplacé d'une disquette à l'autre, d'un ordinateur à l'autre, etc. La saisie de l'immatériel est une notion inconnue en droit de la procédure pénale qu'il importe de consacrer.

9. La **deuxième caractéristique** résulte de la première : la « volatilité » de l'information exprime le fait que celle-ci peut facilement se déplacer, se délocaliser sans cesser d'être immédiatement accessible à travers un réseau. Bref, le « domicile » du délinquant ne s'arrête plus à un lieu physique donné, mais à tout système d'information où celui-ci a eu ou peut avoir virtuellement accès. Dans le monde virtuel, la notion traditionnelle de perquisition attachée à la visite d'un lieu perd donc sa pertinence s'il s'agit d'y découvrir une infraction.

10. La **troisième caractéristique** est « l'opacité » des systèmes d'information, « opacité » voulue par celui qui les utilise et qui protégera l'information confiée au réseau ou à son ordinateur par des procédés de cryptographie, des techniques de sécurité, des codes secrets[22], etc. « Opacité » qui sans doute ne pourra être levée que par la

[19] *Criminalité dans le cyberespace*, Doc. Introductif rédigé par le Conseil de l'Europe à l'occasion de la publication pour discussion du projet de Convention sur la cybercriminalité (Projet n° 19), disponible sur http://convention.coe.int/treaty/frprojets/cybercrime.htm.
[20] A cet égard, l'article de MMrs. H. BRULIN et D. MOREAU, Coopération policière internationale et autorités de contrôle … Mariage d'amour ou de raison, in *Droit des technologies de l'information, regards prospectifs*, E. Montero (éd.), Cahier du CRID, n° 16, Bruylant, Bruxelles, 1999, p. 196 et s.
[21] Ainsi, dans l'actualité récente, l'identification de l'auteur de l'attentat contre le préfet Eyrignac a été réalisé à partir des « traces » digitales laissées par le mobilophone chez l'opérateur du réseau emprunté par la communication téléphonique.
[22] Sur toutes ces techniques de sécurité, lire J. HUBIN, La sécurité informatique, in *La sécurité –Aspects techniques et juridiques*, J. HUBIN-Y. POULLET (éd.), Cahier du CRID n°17, Kluwer, Bruxelles, 1999.

remise des clés ou des éléments nécessaires à l'ouverture du « pli scellé » ou de la caverne d'Ali Baba, ce qui rend nécessaire la collaboration de ceux qui ont aidé à la mise sous clé.

L'opacité peut résulter de la complexité des réseaux que l'information digitalisée emprunte. L'écoute téléphonique était facile dans le monde analogique d'un réseau téléphonique unique connecté. Elle devient impensable lorsque les réseaux se multiplient et que le message tour à tour se fragmente et se reconstitue au hasard des multiples mailles des réseaux. Sans doute, auprès d'opérateurs et d'autres intervenants, des traces de ces messages, de ces utilisations du réseau subsistent-elles Il est tentant dès lors de substituer à la vieille écoute téléphonique, un droit d'accès des autorités policières à ces traces que ces opérateurs et autres intervenants auront eu soin de conserver par ordre légal.

11. Le projet de loi belge prétend donc remédier aux nouveaux risques de criminalité que présente l'utilisation des systèmes d'informations. Ce faisant, le projet répond aux sollicitations internationales pressantes d'une lutte plus efficace contre la criminalité dans le cyberespace. Le Conseil de l'Europe, par le projet de convention « Criminalité dans le cyberespace » qu'il a rendu public le 27 avril 2000[23], préconise en effet : « Les parties (Etats signataires) auront l'obligation d'habiliter leurs administrations respectives à perquisitionner les systèmes informatiques et à saisir des données, à imposer aux personnes concernées de leur fournir les données en leur possession, de conserver les données vulnérables ou de les faire conserver par les personnes concernées ». La possibilité d'intercepter les données transmises par l'intermédiaire de réseaux, y compris les réseaux de télécommunication, est à l'examen. Par ailleurs, les méthodes d'enquête spécifiques à l'environnement informatique nécessiteront la coopération des opérateurs de télécommunication et des fournisseurs de services Internet ; leur aide est en effet vitale pour identifier les délinquants informatiques et établir les preuves de leurs méfaits.

[23] Projet n° 19 établi par le secrétariat à l'attention du Comité européen pour les problèmes criminels et le Comité d'experts sur la criminalité dans le cyberespace,
http://conventions.coe.int/treaty/fr/projets/cybercrime.htm.

SECTION 2 : ANALYSE DES DISPOSITIONS DU PROJET DE LOI A L'ORIGINE DIT N° 214

12. Le principe de régularité des modes de preuve rappelé en exergue de notre propos interdit aux autorités en charge de la poursuite des infractions certains types d'action dans la mesure où ils se heurtent à des principes généraux du droit, comme le secret professionnel, le droit au silence, à la vie privée[24]. C'est ainsi notamment que les écoutes téléphoniques ont longtemps été jugées illégales[25], car contraires à l'article 8 de la Convention européenne des droits de l'homme qui consacre le droit à la vie privée[26] efficacement.

La nécessité de combattre la criminalité favorisée par les technologies de l'information et de la communication a poussé, nous l'avons dit, le législateur belge, comme d'autres[27], à légiférer de manière à légitimer de nouveaux modes de découverte des infractions. Encore faut-il que cette légalisation respecte les principes généraux du droit et que l'exercice de ces prérogatives nouvelles soit circonscrit suivant les mêmes principes. C'est à cette analyse du projet de loi que nous procédons ci-après.

A. La saisie des données

13. L'exposé des motifs du projet de loi justifie comme suit l'introduction d'un nouvel article, l'article 39*bis*, dans le Code d'instruction criminelle.

« La saisie des données pertinentes pour l'instruction, stockées, traitées ou transmises par le biais d'un système informatique, peut s'effectuer intégralement conformément à la procédure traditionnelle dans la mesure où elle s'accompagne de la saisie du support matériel sur lequel elles se trouvent (par exemple, l'ordinateur, des disques optiques, des disquettes …).

Lorsque les autorités judiciaires veulent disposer uniquement des données et ne pas saisir le système informatique ou les autres supports, la situation juridique se présente différemment, principalement parce que la

[24] Sur ces principes et leur application, lire H. BOSLY, « La régularité de la preuve en matière pénale », *J.T.*, 1992, pp. 121 et s.
[25] Sur ce point, la décision de la chambre des mises en accusation de Liège, du 22 septembre 1988, *Pas.*, 1989, II, 47 et le réquisitoire du Procureur général Renaul et les notes signées P.M. et Cass. 2 mai 1990, *R.D.P.,* 1990 , p. 974, note J.S.. Cf. également en doctrine, not., A. MASSET, *op.cit*., pp. 177 et s. ; P. LEMMENS, « het afluisteren van telefoonsgespreken en het registeren van uitgaande en binnenkomende oproepen », *R.W*., 1984-85, col. 1735 à 1739.
[26] … Cette disposition n'autorise « l'ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et des libertés d'autrui ».
[27] Cf. le projet anglais « Regulation of Investigatory Powers Bill », H.L. Bill 61, soumis à la Chambre des Communes le 9 mai 2000 et les textes américains, le premier dit ECPA « Electronic Communications Privacy Act » de 1986, et le second dit CESA, « Cyberspace Electronic Security Act », disponible sur le site du Centre for Democracy and Technology : http://www.cdt.org/crypto/CESA. Nous reviendrons sur ces différents textes.

saisie requiert la soustraction de l'objet en question à celui qui le détient. Par conséquent, la copie de données ne peut pas être assimilée en tant que telle à la saisie d'objets matériels[28].

La nouvelle disposition crée par conséquent une base juridique adéquate pour un nouveau moyen coercitif ayant les mêmes finalités que la saisie. Dans la mesure où aucune dérogation n'est prévue dans cette nouvelle disposition, il est logique que les règles en matière de saisie s'appliquent à la saisie des données »[29].

Des règles particulières sont proposées pour cette saisie : le copiage des données sur des supports *ad hoc* de l'autorité et leur conservation selon des règles de sécurité[30], le blocage de l'accès aux données saisies[31], voire leur retrait dans des cas exceptionnels[32], et surtout l'obligation d'information du « responsable » du système d'information, objet de la saisie.

14. Cette dernière obligation soulève quelques interrogations. Le Conseil d'Etat[33] note l'imprécision du terme. Qui est ce « responsable » ? Le fait qu'il faille l'avertir seulement *a posteriori* soulève la crainte que la saisie puisse se faire à distance, c'est-à-dire sans que le responsable ne soit au courant de la saisie[34]. Ainsi, on peut imaginer que les autorités judiciaires saisissent les données à distance, par exemple en copiant des pages du site du responsable, en s'introduisant dans son système à son insu. Cette question sera réétudiée[35] lorsque seront analysées les dispositions relatives à la perquisition. Ensuite, l'information n'est prévue qu'à propos du responsable et non des tiers concernés par les données saisies, ainsi pourrait être saisie chez le modérateur d'un forum de discussion, la liste des personnes ayant participé à ce forum et les messages émis. On notera que cette information des tiers est préconisée par le Conseil de l'Europe[36] afin de leur permettre d'exercer leurs droits à la levée des actes d'instruction par lesquels ils s'estimeraient liés.

15. Plus fondamentalement, la procédure de saisie des données et non plus - comme traditionnellement - des supports soulève une objection au regard de la règle de proportionnalité. Seuls doivent être saisis les biens qui servent à la manifestation de la vérité et la mesure de la saisie et ses conséquences doivent être en relation avec

[28] Cf. cependant la décision de la Cour d'appel anversoise du 13 décembre 1984, *R.W.*, 1985-86, 244-246 qui admet la saisie de données indépendamment du support.
[29] Exp. des motifs, Doc. Parl. 0213/001, p. 20. Sur la justification de ce passage de la saisie des supports à la saisie des données, lire l'ouvrage collectif du Centrum voor Internationaal Strafrecht (VUB), *Het strafprocedurerecht in gevallen waarbij informatica een essentiele rol speelt*, Kluwer, Informatica en Recht, n°15, Antwerpen – Deventer, pp. 50 et svts et les références y reprises au droit hollandais.
[30] Art. 39 § 6. Il est à regretter que le § 6 n'envisage que les mesures techniques et non celles organisationnelles (gestion des clés d'accès, sanctions disciplinaires). De telles règles techniques et organisationnelles sont nécessaires afin d'interdire les manipulations des données saisies et de préserver l'intérêt des tiers concernés par ces données (cf. sur ce point, les remarques fondées du Conseil d'Etat, avis cité, p. 54).
[31] L'article 39 § 2 alinéa 2 prévoit la possibilité de laisser les données en possession des intéressés pour leur éviter un préjudice, par exemple si les données ou les programmes « saisis » sont nécessaires pour assurer la continuité de l'entreprise.
[32] Le mot « retrait » (des données) n'apparaît pas « s'il s'agit d'un virus qui risque d'endommager le système ou de pages à contenu illicite (art. 39 § 3, al. 2) ».
[33] Conseil d'Etat, avis, *Doc. Parl.* 213/002, p. 54. Le Conseil d'Etat suggère la reprise de la définition donnée par la Recommandation n° R (95) 13 : « Au sens de la recommandation n° R(95)13, *op.cit.*, la notion englobe toutes les personnes qui, lors de la perquisition ou de la saisie, paraissent disposer formellement ou réellement du contrôle sur le système informatique, objet de la perquisition ». Il peut s'agir du propriétaire du système, d'un opérateur de ce système ou même du gardien (locataire ou occupant) des locaux abritant le système informatique. Le Ministre répond à l'objection du Conseil d'Etat que vu la diversité des situations, il est difficile de préciser cette notion.
[34] Certes, prévenir le responsable « avant » voir « au moment de la saisie » lorsque celui-ci est l'auteur ou le complice de l'infraction s'avérerait dangereux dans la mesure où ce responsable risque de faire disparaître ou modifier les informations recherchées mais tel n'est pas le cas lorsque les données visées par la recherche policière et la saisie sont stockées sur l'ordinateur d'un tiers « innocent », responsable du système.
[35] *Infra,* n° 20.
[36] Rapport accompagnant la recommandation n° R(95)13 du Conseil de l'Europe, *op.cit.*, p. 15.

l'enjeu des poursuites et la gravité des faits[37]. La digitalisation de l'information et les infinies capacités de stockage que représente un disque dur voire une simple disquette, justifient la crainte exprimée par la Commission de la Protection de la Vie Privée[38] de voir ce principe appliqué de manière très souple.

On aurait souhaité dès lors, à la suite de la Commission, que la mesure ordonnant la saisie précise bien, d'une part, les personnes soupçonnées et les infractions dont la poursuite requiert la saisie, d'autre part, les raisons pour lesquelles la saisie doit être pratiquée. De plus il faudrait que la saisie soit limitée aux seules données directement en relation avec l'infraction et qu'il y ait au cas où cela n'est pas possible, des mesures strictes d'effacement ou de non utilisation des autres données stockées[39].

B. La perquisition des systèmes d'information

16. L'adaptation du droit de la perquisition aux nouvelles donnes technologiques est sans doute plus complexe encore que celle du droit de la saisie dans la mesure où la perquisition d'un système d'information se heurte, nous l'avons dit (supra n° 8), à la « volatilité » des données. Certaines dispositions du projet répondent à cette préoccupation. D'autres entendent apporter une solution à la « volatilité des données », « l'opacité » des systèmes (supra n° 8).

17. La connexion des systèmes d'information en réseaux et, de ce fait, la facilité de déplacer des données à d'autres lieux physiques comme celle de les utiliser à partir d'autres lieux justifie que la perquisition puisse s'étendre d'un système d'information à un autre, ce qui justifie la dérogation à la règle traditionnelle[40] qui définit chaque mandat de perquisition selon des unités de lieu.

C'est ainsi que l'article 88*ter* nouveau projeté dispose en son § 1 : « Lorsque le juge d'instruction ordonne une recherche dans un système informatique ou une partie de celui-ci, dans le cadre d'une perquisition, cette recherche peut être étendue vers un système informatique ou une partie de celui-ci qui se trouve dans un autre lieu que celui où la recherche est effectuée »[41].

Suivant ce même paragraphe, la décision de cette extension est soumise à certaines conditions : « l'extension doit être nécessaire pour la manifestation de la vérité » et d'autres mesures sont disproportionnées ou un risque

[37] H. BOSLY, D. VANDERMEERSCH, *Droit de la procédure Pénale*, La Charte, 1999, p. 316.
[38] Avis n° 33/99 du 13 décembre 1999 relatif aux projets de loi relatifs à la criminalité informatique (n° 213/1 et n° 214/1) (rapporteurs B. De SCHUTTER et Y. POULLET). Il est à noter que cet avis a été pris d'initiative c'est-à-dire sans que le Gouvernement n'ait pris soin de demander l'avis préalable de la Commission.
[39] A noter cependant qu'ont été insérés dans la mise finale du § 2 de l'article 39bis les mots « qui sont utiles pour les mêmes finalités que celles prévues pour la saisie, qu'indirectement implique un certain contrôle de proportionnalité ». On notera à ce propos la réaction ferme de la Commission exprimée dans l'avis précité.
[40] « L'ordonnance indique le lieu de la perquisition … Il est essentiel que le mandat de perquisition indique de façon précise les lieux visés par la mesure … Les fonctionnaires de police ne peuvent visiter d'autres lieux que ceux repris sur l'ordonnance … ». (H. BOSLY, D. VANDERMEERSCH, *op. cit*., p. 397). On rappellera que toutes saisie ou perquisition opérées en dehors du mandat sont nulles puisque réalisées en dehors du cadre de la saisine du juge.
[41] Comp. l'article 14.2 du projet de convention du Conseil de l'Europe sur la criminalité. « Chaque partie adopte les mesures législatives et autres qui se révèlent nécessaires pour veiller à ce que, lorsque ses autorités perquisitionnent ou accèdent d'une façon similaire à un système informatique spécifique ou à une partie de celui-ci, en recourant aux mesures visées au paragraphe 1(a), et ont des raisons de penser que les données recherchées sont stockées dans un autre système informatique, ou dans une partie de celui-ci, sur son territoire ou en un autre lieu relevant de sa souveraineté, et que ces données sont légalement accessibles à partir du système initial ou disponibles pour ce système initial, lesdites autorités soient en mesure d'étendre rapidement la perquisition ou un moyen d'accès similaire à l'autre système ».

existe que sans cette extension des éléments de preuve disparaissent. On regrettera néanmoins que ces conditions ne doivent pas faire l'objet d'une motivation et que les deux dernières conditions présentées comme une alternative (« ou ») ne soient point cumulatives (« et »)[42].

18. Cette extension est limitée, selon le § 2 du même article du projet, aux systèmes ou parties de systèmes « auxquels les personnes autorisées à utiliser le système qui fait l'objet de la mesure ont spécifiquement accès ». Une telle limitation introduite lors des débats parlementaires[43] se justifie par la crainte de voir les autorités en charge de l'instruction utiliser la nouvelle prérogative que leur donne la loi pour pénétrer l'entièreté du réseau.

Cela signifie que seuls pourront être visités les bases de données, sites, adresses internet, courrier électronique bref les parties du système pour lesquelles une autorisation d'accès a été accordée à la personnes soumise à la perquisition[44]. Ainsi, on peut songer à un compte bancaire accessible par un code secret que messages vocaux ou non déposés dans une boîte électronique au nom de la personne inculpée, à la base de données externe où cette dernière collecte ou range une information partagée avec d'autres, etc. Sans doute, s'agit-il ici d'une définition du domicile « virtuel », c'est-à-dire « de tout lieu où une personne a le droit de se dire chez elle, quels que soit le titre juridique de son occupation et l'affectation donnée aux locaux »[45]. On ajoute que les responsables de ces lieux « à distance » visités doivent faire l'objet en principe d'une information[46].

19. Globalité et caractère international du réseau obligent, cette extension de la perquisition ne s'arrête pas aux frontières du Royaume. Le § 3 alinéa 2 du projet belge contient une solution hardie puisqu'il autorise le juge d'instruction à pénétrer des systèmes situés à l'étranger sans procéder à une demande de commission rogatoire, mais avec un simple devoir d'information *a posteriori* à l'égard des autorités étrangères. Le Conseil d'Etat[47] se

[42] C'est ce que la Commission de la Vie Privée préconisait et que les amendements n° 6 et 15 de Mr. Verheastraeten (*Doc. Parl.* 213/004, p. 2) et de Mr. Poncelet (*Doc. Parl*. 213/005, p. 3) suggéraient. En particulier, le risque de voir disparaître des éléments de preuve devrait en toute hypothèse être démontré. C'est en effet eu égard à ce risque accru par l'utilisation des nouvelles technologies (effacer un fichier est sans doute plus facile et aisé que de brûler des documents papiers) que peut se justifier en définitive la dérogation légale du principe de l'unité de lieu physique de la perquisition.

[43] Suite à l'amendement proposé par Mr. Poncelet (eod. loco) et à la demande de la Commission de Protection de la Vie Privée. L'amendement proposait même l'utilisation des termes : « spécifiquement accès en vertu d'une autorisation particulière ». Le Gouvernement avait défini autrement le critère d'ampleur de l'extension : « la liaison technique par le biais du réseau doit présenter un élément de permanence et de stabilité et ne peut être purement occasionnelle ». Un tel critère était pour le moins flou. La simple répétition de l'accès à une banque de données pouvait dès lors justifier une extension de la perquisition à celle-ci.

[44] Sans doute faut-il rappeler en outre les dispositions valables en matière de perquisitions suivant lesquelles la perquisition doit être limitée strictement à la recherche de l'infraction commise et aux lieux et biens susceptibles de la révéler (Cass. 8 avril 1946, *Pas*., 1946, I, 139, note HAYOIT de TERMICOURT). Le rappel est d'autant plus important que l'intrusion dans un système d'information peut permettre facilement d'avoir une vue de l'ensemble des activités de l'intéressé (courrier échangé, accès à des sites, participation à un forum de discussion, documents stockés, …) et permettrait facilement de détecter des infractions autres que celles pour lesquelles la perquisition a été adonnée. A cet égard on rappellera qu'est illégale la saisie de documents dans des lieux visités et ce lors de la perquisition en dehors du mandat précis (Cass. 6 mars 1944, *Pas.* 1944, I, 237) dans une espèce « ou a été jugée illégale la saisie d'une boîte de saccharine découverte au fond d'un tiroir par des agents des douanes et accises, au cours d'une péremption illégale, parce qu'elle avait été étendue à un tiroir où raisonnablement les agents verbalisants ne pouvaient espérer découvrir des spiritueux et qu'il était dès lors établi qu'ils avaient excéder leur mandat. Mais, poursuit le même auteur, qui cite une nombreuse jurisprudence, si, au cours d'une perquisition, les officiers qui y procèdent venaient à découvrir une infraction d'une autre nature que celle qui donne lieu à leur enquête, sans pour cela excéder les limites de leurs mandat et procéder à des recherches non motivées, ils pourraient et même devraient constater cette infraction et en donner avis au procureur du Roi ». Par contre, il va de soi que la découverte d'une infraction autre que celle à l'origine du mandat, mais sans qu'il y ait eu dépassement du mandat est susceptible d'être constatée (Cass. 29 nov. 1948, *Pas.* 1948, I, 683).

[45] Cf. à ce propos la définition de J. LECLERCQ *in Novelles*, Droit pénal, T. IV, Titre IV, n° 7, 112, p. 125 ; sur cette extension, A. de NAUW, « Recente Tendensen in het onderzoek in strafzaken », *Panoption*, 1988, pp. 217-245, pp. 354 et svts.

[46] Le § 3 excepte de ce devoir d'information les hypothèses « où l'identité et l'adresse de ces responsables ne peuvent être raisonnablement retrouvées…. ».

[47] Le Conseil d'Etat (avis, p. 46) se réfère à cet égard à l'opinion des Etats exprimé dans la recommandation n° R (95)13 déjà cité.

montre particulièrement sévère à cet égard (y voyant « une violation de la souveraineté et du droit international ainsi qu'un contournement partiel de la voie traditionnelle d'entraide judiciaire[48] »).

Le Parlement n'a pas donné suite à ces critiques[49]. Sans doute, l'amélioration des procédures d'entraide internationale préconisée par le récent projet de convention du Conseil de l'Europe[50] et le G 8[51] donnera-t-elle une solution plus respectueuse du maintien des souverainetés nationales tout en étant aussi efficace dans la répression de la cybercriminalité.

20. L'exposé des motifs[52] condamne la pratique suivant laquelle les autorités publiques pourraient « perquisitionner » à partir de leurs propres systèmes d'information et ainsi pénétrer dans ceux d'autrui afin d'y rechercher les éléments susceptibles de constituer la preuve d'une infraction. On connaît ainsi la pratique de certaines polices de se présenter sous un faux nom pour obtenir la preuve d'infractions[53]. En d'autres termes, la perquisition suppose le déplacement physique et non virtuel de l'autorité policière vers le lieu physique où se situe le système d'information d'autrui[54]. La précision est importante. On regrette qu'une telle pratique n'ait pas été plus explicitement condamnée au nom du principe de la régularité des preuves[55].

C. L'opacité des données

21. Le nouvel article 88*quater* projeté répond à la seconde préoccupation : l'opacité des données contenues dans des systèmes d'information. Il permet au juge d'instruction ou l'officier de police judiciaire délégué sur place

[48] Sur cette coopération et entraide policière internationale croissante lire H. BRULIN, D. MOREAU, coopération policière internationale et autorités de contrôle …. Mariage d'amour ou de raison ?, *op.cit*.

[49] Sans doute, le Parlement a-t-il suivi sur ce point le raisonnement du Ministre qui estime : « Par conséquent, le présent projet n'offre pas de réponses unilatérales à toutes les questions qui peuvent se poser en matière de recherche internationale sur réseau. Un certain nombre de points devront indéniablement être traités à l'aide d'instruments internationaux ou en concertation avec d'autres Etats. Néanmoins, les problèmes se posent aujourd'hui et il est dès lors indispensable d'offrir des points d'appui juridiques aux personnes qui, à la suite, d'une recherche dans un système informatique, sont confrontés sur le terrain à la problématique des systèmes informatiques en réseau. Il convient de répondre de manière satisfaisante aux besoins en matière de lutte contre la criminalité sur les autoroutes de l'information.
C'est pour cette raison qua été adoptée, dans le présent projet, une attitude prudente mais pragmatique en la matière. Il est clair que les recherches effectuées en dehors des frontières doivent rester exceptionnelles » (Exp. des motifs, Doc. 0213/001,p. 24).

[50] Cf. le projet de convention n° 19 déjà cité, en particulier les articles 20 et s. L'article 27 n'autorise l'accès transfrontalier à des données stockées à l'étranger sans passer par les procédures d'entraide judiciaire que dans les cas où il s'agit de sites publics ou lorsque la personne responsable du système d'information consent à l'accès ou à la communication des données.

[51] Les travaux du G8 lors de la réunion de Paris récente ont rejeté au nom du principe de souveraineté la proposition américaine de permettre à une cyberpolice d'intervenir partout sans autorisation préalable des Etats concernés. Sur ce point, l'éditorial d'Expertises de juin 2000, « Cybercriminalité – Les Etats conservent leur souveraineté ».
En faveur de cette possibilité d'une investigation transfrontière, S. El ZEIN, « L'indispensable amélioration des procédures internationales pour lutter contre la criminalité liée à la nouvelle technologie », *in Sommet Mondial des Régulateurs*, UNESCO, 30 nov.-1er déc., Rapport, p. 15 : « Les difficultés rencontrées en matière de perquisitions transfrontalières du fait du principe de souveraineté et de l'interdiction de combattre l'illicite par l'illicite commandant la recherche d'une solution qui pourrait consister en un mécanisme international autorisant la perquisition des systèmes informatiques au-delà des frontières nationales, la saisie des données se trouvant sur les réseaux selon des modalités adaptées à l'urgence de la situation. Un tel mécanisme permettrait de rassembler rapidement des données informatiques comme moyens de preuve et reposerait sur des règles déterminant avec précision les conditions d'utilisation par les autorités nationales de police des données ainsi obtenues ».

[52] Exposé des motifs, p. 23. « De même, les services publics ne sont pas autorisés à effectuer, via leurs propres systèmes informatiques, des recherches dans d'autres systèmes non accessibles au public et à propos desquels on suppose qu'ils sont utilisés à des fins criminelles. Par conséquent, l'utilisation par les autorités d'une mesure de surveillance nouvelles et secrète telle que le « hacking » est interdite ».

[53] Dans une investigation menée par le FBI et qui a abouti à l'arrestation d'une douzaine de personnes pour trafic de pornographie enfantine sur l'Internet, la technique utilisée, après localisation de plusieurs sites sur le réseau, sans possibilité d'exercice des pouvoirs coercitifs dans divers Etats des Etats Unis, a consisté pour les policiers à se faire passer pour une fille de 14 ans afin de fixer un rendez-vous à la personne soupçonnée. Libération, « Le FBI fait le ménage sur l'Internet », 21/9/1995.

[54] L'article 87 du Code d'Instruction criminelle dit en effet que « le juge d'instruction se transportera … » « dans le domicile … », mais ne peut-on imaginer que le transport, comme c'est déjà le cas pour le domicile, ne devienne virtuel ?

[55] Sur les limites du droit de la police à s'infiltrer, lire en particulier A. de NAUW, « De Toelaatbaarheid van politie-infiltratie in Belgie, Naar eer en geweten », *Liber Amicorum J. Remmelink*, Arnhem , Gouda Quint, 1987, pp. 452 et s. ; H. BOSLY, « La régularité de la preuve en matière pénale », *J.T.*, 1992, pp. 122 et s.

d'ordonner à ceux qui ont « une connaissance particulière du système informatique qui fait l'objet de la recherche ou des services qui permettent de protéger ou de crypter des données qui sont stockées » de collaborer à la recherche de la vérité. On note que cette collaboration peut prendre diverses formes : fournir les clés de décryptage, les mots de passe, assurer le fonctionnement du système, permettre la copie des données, etc.

Ainsi, l'autorité de certification qui a procédé à l'enregistrement d'une clé publique et fourni le logiciel permettant le cryptage des messages devra fournir à l'autorité compétente les éléments de fabrication de la clé privée, voire aider au décodage des messages signés à l'aide de cette clé. Les services d'archivage des messages révéleront à l'autorité compétente le mot de passe qui permet à l'inculpé perquisitionné d'accéder à sa boite aux lettres électronique. Ces personnes et services seront, ajoute le projet, tenues au secret de l'instruction.

22. Une telle disposition déroge profondément aux principes mêmes de notre droit de la procédure pénale[56] dans la mesure où elle instaure à charge de personnes tierces[57] un devoir de collaboration sous peine, ajoutons le, de sanctions pénales[58]. Certes, dans deux domaines particuliers, le blanchiment d'argent et les écoutes téléphoniques, des lois récentes l'avaient déjà reconnu à charge de certaines professions et pour des opérations précises. L'extension à laquelle il est procédé ici se justifie-t-elle ? Le gouvernement[59] la fonde comme suit : « Dans un contexte de haute technologie en évolution rapide, où il arrive fréquemment que les autorités ne disposent pas de moyens d'expertise suffisants ou que les experts ne soient pas disponibles, il est indispensable de contraindre les personnes ayant une connaissance du système informatique faisant l'objet de la recherche ou ayant une connaissance particulière de certains aspects de ce système (en matière de protection ou de cryptage, par exemple) d'assister les autorités judiciaires.

Il entoure néanmoins la mesure de certaines précautions :

1. le droit au silence de l'inculpé[60] et de ses proches est assuré ;
2. l'ordonnance doit être motivée au regard des circonstances particulières[61].

23. La disposition belge s'inspire de précédents étrangers[62] mais surtout de la Recommandation du Conseil de l'Europe n° R(95)13 qui reconnaît que « Sous la réserve des protections ou privilèges prévus par la loi, les autorités chargées de l'enquête devraient avoir le pouvoir d'ordonner aux personnes qui ont des données spécifiques sous leur contrôle de fournir toutes les informations nécessaires pour permettre l'accès au système informatique et aux données qu'il renferme. Le droit de la procédure pénale devrait assurer que les autorités chargées de l'enquête puissent donner une instruction similaire à d'autres personnes ayant une connaissance du

[56] Comme le reconnaît le gouvernement lui-même : (Exposé des motifs, p. 27). Seuls la procédure par laquelle les tiers peuvent être amenés à témoigner est prévue par la loi. Sur cette procédure et ses limites, lire « Informaticagebeuren en strafvorderingsrecht » (B. De SCHUTTER éd.), *op.cit*., p. 61 et s.

[57] … dont par ailleurs la liste n'est pas précisée et dont certains peuvent être tenues au secret professionnel.

[58] cf. le § 3 de l'article 88*quater*.

[59] Exposé des motifs, p. 27.

[60] Sur ce principe, notamment, P. QUARRE, « Le droit au silence », *J.T*., 1974, pp. 524-528 ; M. FRANCHIMONT, « Les droits de la réalité, Les droits de la défense en matière pénale », *Actes du colloque des 30-31 mai-1er juin 1985*, Barreau de Liège, ASBL, Ed. Jeune Barreau, 1985, p. 42. Ce droit a été consacré par l'article 14(g) de la loi du 15 mai 1981.
On ajoute que ce droit au silence ne vaut pas pour une personne morale (Arrêts de la Cour de Justice du 18 nov. 1989, Affaire Orkun (374/87) et Solvay (27/88)). Un organe ou un préposé de l'entreprise inculpé ne pourront dès lors se prévaloir de ce droit au silence.

[61] Suivant la formulation proposée par l'amendement de Mr. VERHERSTRATEN (*Doc. Parl.* 0214/005, p. 752). A l'origine, le texte ne prévoyait pas cette obligation.

fonctionnement du système informatique ou de toute mesure employée pour préserver les données y contenues »[63].

Récemment, les Etats-Unis ont introduit un projet de loi : le « Cyberspace Electronic Security Act » (en abrégé CESA)[64] qui oblige les « Recovery Agents », c'est-à-dire tous les services intervenant dans l'émission ou la conservation[65] des clés de décryptage, à transmettre aux autorités judiciaires compétentes, les moyens de régénérer la clé ou de décrypter les messages signés à l'aide de la clé.

24. L'intérêt de ce texte pour notre propos est triple :

1) Le texte législatif américain concerne une catégorie professionnelle précise. Le texte belge pêche par l'imprécision[66] des acteurs visés. Il pourrait s'agir aussi bien de certificateurs intervenant en matière de signature électronique, des fournisseurs d'accès à Internet, des fournisseurs de services, des sociétés d'archivage, des banques et généralement de toute entreprise qui offre un service destiné à assurer la sécurité de la création, de la conservation ou de la transmission d'informations ;

2) Quatre conditions sont mises à l'accès des autorités policières[67], conditions qu'on aimerait retrouver dans le texte belge : la première porte sur la nécessité de la mesure pour l'accès à l'information ; la deuxième porte sur le respect des conditions de légitimité de l'ordre ; la troisième sur la durée de l'accès[68] et enfin, la quatrième porte sur l'interdiction de violer l'atteinte légitime raisonnable *(constitutionnaly protected expectation of privacy*) de la vie privée de l'inculpé ou si, tel est le cas, de l'obligation de peser l'intérêt protégé par cette atteinte et les raisons invoquées par la décision d'ordonner l'accès. Ces quatre conditions sont vérifiées préalablement à la décision en fonction de « *specific and articulable facts* ». La décision doit être motivée[69] sur ce point et la personne visée par la mesure doit pouvoir être entendue[70].

---

[62] En particulier, la loi hollandaise. Sur cette loi, lire « Informaticagebeuren en Strafvorderingsrecht » (B. De SCHUTTER), *op. cit*., p. 64 et s.

[63] Les articles 14 et 15 du projet de Convention du Conseil de l'Europe sur la cybercriminalité disposent de manière plus précise :
Art. 14.5 : « Chaque partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes, pour les besoins d'enquêtes et de procédures pénales, à enjoindre à toute personne connaissant le fonctionnement du système informatique ou les mesures appliquées pour protéger les données informatiques qu'il contient de fournir toutes les informations raisonnablement nécessaires, pour permettre l'application des mesures visées par les paragraphes 1 et 4.
Art. 15.1 : « Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à enjoindre à une personne présente sur son territoire ou en un autre lieu relevant de souveraineté de fournir des données informatiques spécifiées qui sont sous le contrôle de cette personne et sont stockées dans un système informatique (ou un support permettant de stocker des données informatiques) sous la forme requise par ces autorités, pour les besoins de l'enquête et de procédures pénales.

[64] Sur ce projet dans ces diverses versions et les critiques que le Center for Democracy and Technology lui adresse, cf. http://www.cdt.org/crypto/CESA.

[65] Il est constaté que l'utilisation de ces services se généralisent tant la perte d'une clé, suite à un oubli , à un vol ou à un décès, peut s'avérer catastrophique pour une entreprise ou une personne.

[66] Cette remarque rejoint les critiques du Conseil d'Etat et de la Commission de la Protection de la Vie Privée.

[67] Cf. la section 2712(b) du *Bill* américain.

[68] Cette condition vise clairement à interdire l'utilisation prolongée des clés de décryptage par les autorités.

[69] Il est assez remarquable de constater que la loi belge du 30 juin 1994 insérait un article *90quater* au Code d'Instruction criminelle autorisant les écoutes téléphoniques prévoyait des conditions semblables à l'ordonnance du juge autorisant l'écoute. L'ordonnance devait être motivée, démontrer le caractère indispensable, indiquer les indices justifiant la mesure, définir la personne, le moyen de télécommunication et le lieu surveillé, la durée de l'écoute, le nom de la personne habilitée à la pratiquer. Il est regrettable que de telles précisions n'aient pas été reproduites dans le contexte du présent projet.
Sur ces limites, lire Th. HENRION, « Les écoutes téléphoniques », *J.T*., 1995, p. 210.

[70] Le projet anglais (*regulation of Investigatory Powers Bill*, version du 10 mai 2000) disponible sur http://www.parliament.the-stationery-office.co.uk/pa/ld199900:ldbells/061/00061—a.htm) prévoit dans sa partie III : « *Investigation of Electronic data protected by encryption key* » que le droit de demander la levée de clé n'est légitime que si « on reasonable grounds », la personne habilitée à la demande estime « *(a) that a key to the protected information is in the possession of any person,*

3) Enfin, le texte justifie la mesure exceptionnelle consacrée par le *bill.* Elle apparaît clairement comme une contrepartie au droit de chacun d'utiliser les techniques d'anonymat et de cryptographie[71] sans crainte d'une violation de l'anonymat et de la confidentialité par des techniques policières secrètes[72].

… Un problème particulier : Perquisitions et secret professionnel

25. La balance d'intérêts prévue entre l'attente de la personne soupçonnée au respect de sa vie privée et l'intérêt public poursuivi par l'autorité policière dans sa recherche d'infractions commises conduit notamment à la prise en considération de la qualité de celui qui détient les clés, en particulier lorsque celui-ci est tenu par le secret professionnel.

La Commission de la Protection de la Vie Privée[73] avait mis en évidence ce problème particulier, dans la mesure où la personne appelée à collaborer devrait pouvoir invoquer ce secret pour s'opposer à toute mesure[74] et, lors d'une perquisition, devrait pouvoir réclamer quelques garanties (présence d'un membre du Conseil de l'Ordre de la profession) pour limiter strictement sa collaboration au système d'information.

> « Par ailleurs, la Commission souhaite attirer l'attention du législateur sur le fait que les textes en projet ne règlent pas la question de savoir dans quelle mesure certains responsables de systèmes informatiques pourront invoquer la règle du secret professionnel (avocats, journalistes, médecins …). Rien n'est prévu pour que les personnes astreintes au secret professionnel puissent l'invoquer. Les précautions particulières qu'impliquent la sauvegarde du secret professionnel face à une perquisition nécessitant l'accès à un système informatique devraient également être réglées. La Commission est d'avis que des mécanismes d'intervention des instances professionnelles devraient être légalement prévus. Ainsi, on pourrait imaginer qu'un membre du Conseil de l'Ordre des médecins ou des avocats soit présent lors de l'intervention des autorités judiciaires ».

(b) that the imposition of a requirement to disclose the key is – (i) necessary on grounds falling within subsection, or (ii) likely to be of value of purposes connected with the exercise or performance by any public authority of any statutory power or statutory duty,
(c) that the imposition of such a requirement is proportionate to what is 15 sought to be achieved by its imposition, and
(d) that the key cannot reasonably be obtained by the person with the appropriate permission without the giving of a notice under this section,
the person with that permission may, by notice to the person whom he 20 believes to have possession of the key, require the disclosure of the key ».
La personne requise peut s'opposer à la demande, suivant le même projet.
A person shall not give a direction for the purposes of subsection unless he believes
(a) that there a special circumstances of the case which mean that the purposes for which it was believed necessary to impose the requirement in question would be defeated, in whole or in part, if the direction were not given ; and
(b) that the giving of the direction is proportionate to what is sought to be achieved by prohibiting any compliance with the requirements in question otherwise than by the disclosure of the key itself.

[71] A cet égard, on note le point (i) des Findings du Bill, repris à la Sect. 102. « *A sound and effective public policy must support the development and use of encryption is utilized by criminals. Law enforcement entities have a critical need to decrypt communications and stored data that they are lawfully authorized to access in order to obtain the plaintext that is necessary to conduct investigations and prosecutions of such unlawful activity, and there is a compelling national interest in preserving law enforcement entities' ability to obtain such plaintext. Appropriate means must be available to fulfill these law enforcement objective, consistent with existing legal authorities and constitutional principles, in order to protect public safety. This requires an approach which properly balances critical privacy interests with the need to preserve public safety* ».

[72] « *CESA no longer includes « secret search » authority allowing government agents to secretly break into people's homes and install « recovery devices » on their computer if they did not use key recovery. The bill also no longer contains other provision to promote the use of key recovery* ». (cf la déclaration du Center for Democracy and Technology, disponible à http://www.cdt.org/publications/pp. 5-22.html).

[73] Avis de la Commission, *op.cit*., p. 4.

[74] C'est la solution retenue par la loi néerlandaise.

26. En ce qui concerne le droit de perquisitionner le système d'information d'un professionnel de la santé, on rappellera que la jurisprudence de la Cour européenne des droits de l'homme[75] exige sur base de l'article 8 de la Convention que les locaux abritant des documents couverts par le secret professionnel jouissent d'une protection accrue, que toute perquisition en la matière soit proportionnée[76] et ciblée, de manière à éviter l'accès à des documents couverts par le secret professionnel étrangers à l'enquête[77]. La présence ou au moins l'information d'un représentant autorisé de la profession (un membre du Conseil de l'Ordre) sont en outre requis[78].

27. En ce qui concerne le devoir de collaboration, le Conseil d'Etat avait clairement plaidé pour une exception « sous peine de vider l'article 458 du Code pénal de tout sens »[79].

Sans que le texte ne mentionne expréssement une exception au profit des dépositaires de secret professionnel, on notera cet étrange passage de l'exposé des motifs[80] : « En ce qui concerne les personnes tenues au secret, le but n'est pas de déroger au droit commun en matière de respect du secret professionnel : les personnes tenues par le secret professionnel et agissant dans le cadre du secret professionnel suivent le même régime que si elles étaient appelées à témoigner en justice ; ceci implique donc un droit et pas une obligation de coopération lorsqu'elles doivent rechercher elles-mêmes des données spécifiques ».

Ainsi, les personnes tenues au secret professionnel seraient-elles en droit de se taire et de ne pas collaborer. Une telle conclusion apparaît comme illogique dans la mesure où ce droit de se taire est copié selon les dires du Ministre de celui existant au profit de ces personnes lorsqu'elles sont appelées à témoigner[81]. Et l'appel au témoignage du dépositaire d'un secret en réponse à des assertions formulées est bien différent de l'appel à la collaboration dans la recherche d'une infraction par la mise en œuvre de moyens propres à ce dépositaire.

D. Des écoutes téléphoniques, de l'interception de messages et finalement de l'obligation à leur conservation

28. Par touches progressives[82], le législateur belge complète l'arsenal des mesures susceptibles d'être prises par les autorités policières pour surveiller les communications qui toujours plus variées empruntent nos réseaux de télécommunications modernes.

---

[75] A ce propos, CE.D.H. 16 déc. 1992, *Rev. trim. D.H.*, 1993, p. 467, note P. LAMBERT et F. RIGAUX, ; CEDH, 25 mars 1998, *Journ. des Proc.,* 17 avril 1998, p. 22 (à propos d'écoutes téléphoniques).

[76] Cf. la note de E. JAKHIAN et P. LAMBERT, « Les perquisitions dans les cabinets d'avocats », sous CEDH, 16 déc. 1992, *J.T.*, 1994, p. 65.

[77] A ce propos H. BOSLY et D. VANDERMEERSCH*, op. cit.*, p. 400.

[78] Cf. à ce propos le débat entre la tendance dure de P. LAMBERT (*Le secret professionnel*, Bruxelles, Némésis, 1985, pp. 176-177) et celle plus souple d'I. VIAENE (Huiszoeking en beslag in strafzaken, *A.P.R.*, Bruxelles, Larcier, n° 485-489).

[79] Avis du Conseil d'Etat, p. 55.

[80] Exposé des motifs, p. 28.

[81] A propos du droit du dépositaire du secret à se taire lors de leur interpellation à témoigner, lire not. C. HENNEAU-VERHAEGEN, « Recherche Policière et secret médical », *JT*, 1988, pp. 165 et s.

[82] - Loi du 11 fév. 1991, insérant un art. 88*bis* dans le Code d'instruction criminelle, *M.B.*, 16 mars 1991 (à propos du repérage des communications)

- Loi du 30 juin 1994 relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées, *M.B.*, 24 janv. 1995.
- Loi du 19 décembre 1997 modifiant la loi du 21 mars 1991, *M.B.*, 30 déc. 1997.
- Loi du 10 juin 1998 modifiant la loi du 30 juin 1994.

A propos des législations qui ont précédé le projet actuel, bien des articles ont paru[83]. Nous ne reprenons ici que les nouveautés introduites par le projet actuellement en débat.

29. La loi élargit de la liste des infractions pour lesquelles une mesure d'écoute peut être opérée par la modification projetée de l'article 90*ter* § 2. Cet élargissement concerne des infractions déjà reconnues par des lois préexistantes, ainsi les écoutes illégales en matière de télécommunications visées par les articles 259*bis* et 314*bis* du Code pénal. Il couvre également les nouveaux délits envisagés par le projet de loi : ainsi, le faux en informatique (futur article 210*bis* du Code pénal) et finalement les « infractions contre la confidentialité, l'intégrité et la disponibilité des systèmes informatiques et des données qui sont stockées, traitées ou transmises par le biais de ces systèmes » (futurs articles 550*bis* et 550*ter* du Code pénal).

Il se justifie par le fait que la commission de ces délits dits de criminalité informatique s'opère souvent par les réseau. Par ailleurs, ces délits illustrent, à l'instar des délits importants pour lesquels l'écoute était déjà permise, la vulnérabilité de notre société dite de l'information face aux diverses formes de délinquance informatique[84].

30. Le projet de loi relatif à la criminalité informatique traitent de la collaboration de divers acteurs à la recherche d'infractions par les autorités policières. Elles s'inspirent des devoirs de collaboration déjà mentionnés à propos des perquisitions et prolongent ceux déjà admis par les lois de 1994 et de 1997 sur lesquels nous reviendrons.

31. Deux types de collaboration sont essentiellement prévus. Un nouveau § 4 complète l'article 90*quate*r qui, depuis la loi de 1994, autorise les mesures d'écoute mais les soumet à une ordonnance motivée du juge d'instruction[85]. La seule collaboration prévue alors était d'ordre technique : il s'agissait pour les opérateurs de

---

[83] Cf. notamment les études suivantes : Informaticagebeuren en Strafvorderingsrecht (*M.B*., 22 sept. 1998, B. De SCHUTTER éd.), *op. cit*., pp. 69-97 ; H.D. BOSLY et D. VANDERMEERSCH « La loi belge du 30 juin 1994 relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées », *rev. dr. Pén*, 1995, pp. 301-343 ; Th. HENRION, « Les écoutes téléphoniques », *J.T*., 1995, pp. 205-213 ; L. HUYBRECHTS, « het gerechtelijk afluisteren in het belgisch recht na de nieuwe afluisterwet », *Panopticon*, 1995, pp. 41-57 ; Ph. TRAEST, « Analyse van de wet van 30 juni 1994 », Telefoontap,, Leuven, 1997, p. 2-26 ; D. VANDERMEERSCH, Les modifications en matière de repérage et d'écoute de (télé)communications introduites par la loi du 10 juin 1998, Rev. dr. Pén. Crim., 1999, p. 1061.1074. ; F. GOSSENS, Wanneer mag een telefonisch gesprek opgenomen en beluisterd worden ? Over art. 314 bis § 1, 1° SW, *A..J.T*., 1999-2000, pp. 235 et svts.

[84] Ceci dit, on s'inquiète du nombre d'infractions reprises à l'article 90*ter* et pour lesquelles la mesure d'écoute est permise. Il deviendra de plus en plus difficile de nier le droit de l'autorité à procéder à l'écoute tant le nombre d'infractions susceptibles de la légitimer est important (cf. à cet égard, les remarques du Rapport de la Commission de Justice du Sénat à propos de la future loi de 1994 où les rapporteurs insistaient sur la nécessité de n'utiliser l'écoute que pour l'élucidation de faits relevant directement d'une des (rares à l'époque) infractions visées par le texte.

[85] Le prescrit légal prétend répondre aux exigences du principe général du droit au respect de la vie privée. Selon ce principe, une interception ne peut être admise que si elle répond à trois exigences fondamentales, conformément à l'article 8 § 2 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales du 4 novembre 1950, et de l'interprétation réservée à cette disposition par la Cour européenne des droits de l'homme : une base légale, la nécessité de la mesure dans une société démocratique et la conformité à l'un des buts légitimes énumérés dans la Convention. La loi devra définir précisément les limites et les modalités de son exercice au moyen de règles claires et détaillées qui sont surtout nécessaires en raison du perfectionnement continu des moyens techniques utilisables. Ce texte de loi doit être accessible au public afin que le citoyen puisse prévoir les conséquences de son comportement.
La Convention n° 108 du Conseil de l'Europe prévoit également qu'une mesure d'ingérence n'est tolérée que lorsqu'elle est strictement définie au regard de cette finalité. A ce titre, la surveillance exploratoire ou générale effectuée sur une grande échelle doit être proscrite. (Sur ces diverses limites, Th. HENRION, *op. cit*.).
On appréciera sur ce point la manière dont C. GUERRIER et M.C. MONGET *(Droit et Sécurité des télécommunications*, coll. Techniques et Scientifique des Télécommunications, Springer Verlag-CENT ; Paris, 2000, p. 99 et s.) résument la position française.
Dans toutes les circonstances, l'écoute judiciaire, atteinte à la liberté individuelle, ne pourra être envisagée que si les autres moyens d'investigation sont inefficaces. Il ne convient pas de banaliser un procédé hors normes. Le formalisme sera précis : la motivation sera obligatoire ; la mise sous surveillance sera temporaire. Les enregistrements, s'ils permettent la manifestation de la vérité, seront utilisés.

réseaux de prêter leur concours technique au branchement des autorités policières et ce afin de permettre la réalisation de l'écoute. Le § 4 introduit une obligation de collaboration d'une toute autre portée. Il ne s'agit plus de viser seulement les opérateurs des réseaux peu importe la technique de réseau (réseau mobilophonique, réseau satellite, réseaux cablés y compris les réseaux de télédistribution), mais surtout les fournisseurs des services de télécommunication qui empruntent ces réseaux : services de cryptographie, d'accès à Internet, services de messagerie, voire de simple transport.

Vis-à-vis de ce cercle singulièrement élargi, le juge peut ordonner, sous peine de sanctions pénales, leur collaboration pour accéder au contenu de la télécommunication sous forme compréhensible. A leur charge, pèse une obligation de moyens et ces personnes seront tenues de respecter le secret de l'instruction. On retrouve ici l'esprit et le contenu des dispositions déjà analysée à propos des perquisitions[86]. Sans doute, fallait-il tenir compte du fait que les réseaux, désormais digitalisés et non plus analogiques, et l'utilisation de techniques de cryptographie auraient rendus inefficaces la simple écoute prévue jusqu'ici[87]. Ceci dit, la disposition inquiète dans la mesure où l'ordonnance prévue par le paragraphe 4 si elle s'ajoute à l'ordonnance prévue par le paragraphe 1er ne reprend cependant pas les mêmes conditions très strictes fixées par ce paragraphe[88].

32. Cette obligation de collaboration des opérateurs de télécommunications et des prestataires de services de télécommunications est encore élargie par le complément que le projet insère à l'article 109*ter* E de la loi du 25 mars 1991 portant réforme de certaines entreprises publiques dont on note qu'il a déjà été modifié à de multiples reprises[89] . Il s'agit, une nouvelle fois, sous peine de sanctions pénales, d'astreindre les opérateurs de réseaux et les fournisseurs de services de télécommunications à conserver en Belgique[90], dans certains cas qui restent à déterminer par arrêté royal et pendant une durée maximale de 12 mois[91], les données d'appel de moyens de télécommunications et les données d'identification d'utilisateurs de services[92].

Dans le cas contraire, ils seront détruits. La violation du secret professionnel, l'ingérence inutile dans la vie privée, seront évitées. Les écoutes judiciaires seront reproduites dans les registres tenus par les livres de police judiciaire.

[86] Cf. *supra* n° 21.

[87] L'obligation de collaboration « techniques » des opérateurs à l'exécution de mesures judiciaires d'écoute est certes préférable à des solutions plus dangereuses encore pour la protection des données : ainsi, l'interdiction de cryptographie, ou le dépôtdes clés obligatoires (recovery ou key escrow) auprès d'une autorité publique (Cf. la défunte proposition américaine du Clipper chip I) oucd'un tiers auprès duquel les autorités publiques peuvent s'adresser (cf. la défunte proposition américaine du Clipper Chip II). Sur ces diverses possibilités et la préférence en faveur de la solution de collaboration, lire l'avis très détaillé de la Commission de Protection de la Vie Privée (Rapporteur B. De SCHUTTER, n° 17/1997 du 9 juillet 1997).

[88] C'était déjà le cas en ce qui concerne les ordonnances de saisies. Nous avions regretté sur ce point le silence du législateur de l'an 2000 (cf. *supra* n° 15).

[89] L'article 109*ter* a été inséré par la loi de 1994 et modifié profondément par la loi du 10 juin 1998.

[90] Une telle disposition est, à notre avis, contraire au principe de libre circulation des services et de libre établissement consacré par les traités de l'Union européenne. Elle a été introduite lors des discussions parlementaires par le député VERHERSTRAETEN (*Doc. Parl*. 214/004, p. 3) au motif que « Certains fournisseurs d'accès à l'Internet en Belgique conservent leurs fichiers à l'étranger. Cela pose fréquemment des problèmes en matière de recherche et de dépôt au niveau international. C'est la raison pour laquelle nous proposons que la conservation doive impérativement s'effectuer dans les limites du territoire national ».

[91] La première version du projet laissait au Roi le soin de déterminer ce délai. Nonobstant les remarques de la Commission de Protection de la Vie Privée (Avis n° 33/99 du 13 décembre 1999 relatif aux projets de loi relatifs à la criminalité informatique) relayées par l'amendement PONCELET *(Doc. Parl.* 214/005, p. 4) et fondées sur l'avis du Groupe européen dit de l'article 29 de Protection des données (Recommandation n° 3/99 du 7 sept. 199 relatif à la préservation des données de trafic par les personnes de services Internet pour le respect du droit) de limiter ce délai à 3 mois, le Parlement fixa ce délai à 12 mois minimum. Le Sénat le ramena à 12 mois maximum. On ajoutera que les législations allemandes et néerlandaises fixent à 3 mois cette durée de conservation.

[92] On notera que la Commission de Protection de la Vie Privée est appelée à se prononcer par avis à propos de la durée de conservation et de la nature des données à conserver. Par exemple, à props des utilisations du navigateur. S'agit-il de conserver trace de l'ensemble des caractéristiques de telles utilisations (adresse des sites visités, durée de la visite, pages visitées, itinéraire suivi) ou se contentera de données plus élémentaires. On notera à ce propos l'avis de la Commission de Protection de la Vie Privée (avis n° 09/97 du 20 mars 1997 à propos du projet de loi concernant l'identification et le repérage des numéros de postes de communication ou de télécommunication et portant modification des articles 90*ter*, 90 4°, 90 6° et 7° du Code d'Instruction Criminelle) : La Commission reconnaît qu'aur egard de l'évolution des technologies, la collaboration des opérateurs de réseaux de télécommunications et des fournisseurs de services, sera dorénavant requise pour rendre efficace les mesures ordonnées. Elle attire cependant l'attention du législateur sur le fait qu'une telle collaboration peut créer des

33. Ce complément suscite de nombreuses craintes. On rappellera que la disposition légale proposée complète une disposition récemment modifiée. Il s'agit de la loi du 11 juin 1998 modifiant la loi du 30 juin 1994 relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées. Cette disposition veut que le Roi détermine, après avis de la Commission de la Protection de la Vie Privée, par arrêté délibéré en Conseil des Ministres, « les moyens techniques par lesquels les opérateurs de réseaux et les fournisseurs de services de télécommunications doivent permettre le repérage, la localisation, les écoutes, la prise de connaissance et l'enregistrement de télécommunications privées »[93].

La crainte principale[94] exprimée à l'égard de cette loi était l'instauration d'une surveillance exploratoire générale en particulier dans la mesure où les autorités judiciaires recevaient le droit d'extraire des banques de données tenues par les opérateurs et fournisseurs de services des informations permettant une surveillance générale et exploratoire. Cette surveillance générale est bannie par les principes mêmes établis par la Cour européenne des Droits de l'Homme sur base de l'article 8 de la Convention européenne[95].

L'ajout d'un § 2 à l'alinéa 1er amplifie considérablement les moyens donnés à l'autorité policière puisqu'il s'agit de leur permettre d'accéder aux données de communication non seulement en temps réel mais également en temps différé. En effet, est mise à charge des prestataires de services de télécommunication l'obligation de mettre à disposition des autorités les données conservées pendant « au maximum » 12 mois.

34. La signification concrète d'une telle obligation mérite d'être examinée :

- notons qu'elle vise tout « fournisseur de services de télécommunications », c'est-à-dire non seulement les services traditionnels de transport des communications, mais également les multiples prestataires intervenant dans l'offre de services internet (services d'accès, services de messagerie, services de forum de discussion, etc.) ou dans l'offre de services à valeur ajoutée (services de cryptographie, services de Trusted Third Parties, services électroniques bancaires, …). Bref, chacun de ces prestataires sera tenu de conserver pendant 12 mois au moins les multiples traces laissées par l'utilisation des réseaux. On notera à la suite de J.M. Dinant[96] que ces traces sont, du fait de l'informatisation croissante de tous les secteurs, « de plus en

---

risques nouveaux d'atteinte à la vie privée, dans la mesure où la réponse aux demandes de l'autorité publique peut requérir des traitements nouveaux dans le chef des opérateurs et fournisseurs. Ces traitements nouveaux doivent être identifiés et soumis aux règles de proportionnalité, en particulier, la durée de conservation des données opérées dans le cadre de ces traitements doit être précisée, et les utilisateurs de ceux-ci définis.

[93] Un premier projet d'arrêté royal déterminant ces « moyens techniques » avait fait l'objet de vives critiques de la Commission (avis n° 12/99 du 24 mars 1999). Un second projet d'arrêté royal est actuellement à l'étude.

[94] Cf. à ce propos l'avis de la Commission de Protection de la Vie Privée n° 09/97 du 20 mars 1997 (Rapporteurs B. DE SCHUTTER et Y. POULLET) qui notait : « Au regard de telles considérations et dans la mesure où l'article 22 de la Constitution rappelle la nécessité de mesures législatives pour toute dérogation au principe du respect de la vie privée, la Commission ne peut admettre que la matière soit réglée par une délégation à un arrêté royal, sans que ne soient fixées les limites strictes de cette intervention royale. La Commission rappelle, en particulier, que de telles mesures techniques ne peuvent avoir pour effet de légitimer les pratiques de repérage ou d'interception préventives, qu'elles ne peuvent conduire les autorités publiques à disposer d'informations disproportionnées par rapport à celles nécessaires dans le cadre de l'instruction, enfin qu'elles doivent respecter le caractère strictement d'exception de l'écoute ».

[95] Ce principe est mis en exergue par les Recommandations du Groupe dit de l'article 29 concernant le respect de la vie privée dans le contexte de l'interception des télécommunications (Recommandation 2/99 du 3 mai 1999 doc. 5005/99 final W.P. 18) et relative à la préservation des données de trafic par les fournisseurs de services Internet pour le respect du droit (Recommandation n° 3/99 du 7 septembre 1999).

Ces recommandations sont disponibles sur le serveur de l'Union européenne, http://europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/

[96] In Y. POULLET-J.M. DINANT, Le réseau Echelon, Existe-t-il ? Que peut-il faire ? Peut-on et doit-on s'en protéger, Rapport d'expertise rédigé à l'attention du Comité Permanent de contrôle des services de renseignements, mai 2000, Doc. confidentiel, p. 6 ; cf. du même auteur

plus nombreuses, que le détenteur, la nature et le lieu du stockage de ces traces deviennent de moins en moins visibles par l'individu qui le laisse le plus souvent malgré lui ». Que l'on songe à la visite d'un site Web proposé par un serveur quelconque et ce à partir du site d'une société fournisseur d'un service d'indexation automatique *(search engines*) comme Lycos ou Anastasia, l'internaute laissera, sans compter les nombreux traitements invisibles possibles[97], des traces chez le ou les opérateur(s) des réseaux de télécommunications que son message empruntera, chez le fournisseur d'accès et chez les différents serveurs des sites visités.

- la nature des traces laissées dans l'exemple donné est variée. Si l'opérateur de réseau garde les traces du trafic (le numéro appelant ou plutôt l'adresse d'origine du message, la durée de connexion ou la longueur et le numéro appelé ou plutôt l'adresse du destinataire du message), le fournisseur d'accès peut dans son *logbook* conserver la trace des diverses utilisations opérées à partir du système d'information de l'internaute: les différents sites visités, voire les pages visitées et le parcours suivi, la durée de chaque visite et bien évidemment les caractéristiques de la configuration utilisée par l'internaute. Une même richesse d'information se retrouvera chez l'opérateur du service de recherche et d'indexation automatique, etc.[98]

35. Comme le note la Commission de la Protection de la vie privée[99], le texte en projet contraint les fournisseurs de services à enregistrer toutes ou certaines de ces données qu'ils n'enregistreraient pas forcément pour la mise en œuvre de leurs services[100].

Certes, la loi laisse dans le vague les données à conserver et confie au Roi le soin d'en dresser la liste. On peut espérer que cette liste soit minimale et strictement proportionnée aux besoins de constatation *a posteriori* de l'infraction (ainsi, par exemple les seuls émetteurs et destinataires), mais, en toute hypothèse, il eût été conforme aux exigences de la Cour Européenne des Droits de l'Homme que ce soit la loi même qui précise cette liste de manière détaillée afin que chaque citoyen puisse à partir de la lecture du texte fixer son comportement[101] « la loi doit user de termes assez clairs pour indiquer à tous de manière suffisante en quelles circonstances et sous quelles conditions elle habilite la puissance publique à opérer pareille atteinte au respect de la vie privée ». La Cour précise en plus que les écoutes « doivent se fonder sur une loi d'une précision particulière et que

---

[97] A cet égard, l'excellent rapport de J.M. DINANT, rapport rédigé pour le projet européen ECLIP, disponible à http://www.droit.fundp.ac.be/textes/privacy_law_tech_convergence.rtf.

[98] On note à la suite de l'avis de la Commission de la Protection de la Vie Privée, « le champ d'application est très large : les données visées ont trait à quiconque utilise des services de télécommunication. Il s'agit potentiellement de toute la population ; et l'ensemble des services de télécommunication est couvert. En effet, dans notre société qui évolue de plus en plus vers une « société de l'information », l'utilisation des services de télécommunications occupe une place grandissante.
En outre, les catégories de données ne sont pas circonscrites de manière précise (cf. l'exposé des motifs, qui ne contribue pas à la clarté en mentionnant a priori certaines données sans exclure les autres de manière définitive) ».
Ainsi, par exemple les données relatives aux sites consultés par un internaute ne devraient être conservées que dans certaines situations « exceptionnelles ». En outre, d'autres données a priori exclues, comme la localisation en cas d'utilisation d'un GSM seront généralement conservées jusqu'au moment où la facturation ne peut plus être contestée. On ne peut dès lors exclure de manière définitive leur communication aux autorités durant ce délai.

[99] Avis ….. *op.cit*., p. 9.

[100] Allons plus loin, selon les principes de la loi vie privée et en particulier le principe de proportionnalité, l'enregistrement de ces données et en tout cas leur durée de conservation seraient sévèrement limités voire interdits dans la mesure où rien ne justifie (par exemple, si le service est gratuit) la conservation des données.

[101] Il importe « que ces finalités soient prévues par la loi, c'est-à-dire par un texte réglementaire accessible au public et rédigé de façon suffisamment précise pour que le citoyen puisse y répondre par un comportement adéquat » (Arrêt Malone, 2 août 1984, série A, n° 82 ; Arrêt Kruslin, 24 avril 1990, Série A, n° 166-A et n° 176).

* NdA : Nous soulignons

l'existence de règles claires et détaillées en la matière apparaît indispensable, d'autant que les procédés techniques utilisables ne cessent de se perfectionner »*[102].

36. Une obligation de conservation et de divulgation rapide des données relatives au trafic est aussi prévue par le texte en projet de Convention du Conseil de l'Europe[103]. L'expression utilisée par l'instance internationale reste très prudente :

« 1. Pour mettre en œuvre les procédures visées par l'article 16 en vue de la conservation de données relatives au trafic concernant une communication spécifique, chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour :

a) veiller à la conservation rapide de ces données relatives au trafic, indépendamment de la question de savoir si un seul ou plusieurs fournisseurs de service ont participé à la transmission de cette communication et

b) assurer la divulgation rapide à l'autorité compétente de la Partie, ou à une personne désignée par cette autorité, d'une quantité suffisante de données relatives au trafic aux fins d'identification des fournisseurs de services et de la voie par laquelle la communication a été transmise.

c) Les prérogatives et les procédures visées par le présent article sont subordonnées aux conditions et garanties prévues par le droit interne ».

On note que la mesure est liée à la recherche d'une communication spécifique, que la conservation ne peut être que de courte durée et que ces procédures obéissent aux garanties du droit interne. A cet égard, on note que le projet de loi anglais dans sa seconde partie insiste sur l'importance des tests de nécessité : « la mesure d'investigation permise par cette conservation des données doit être « nécessaire » au regard de l'intérêt public majeur à défendre » ; et de proportionnalité : « les données à obtenir doivent être proportionnées par rapport à ce qui est recherché à travers la mesure d'investigation »[104].

Le Conseil des Ministres de l'Union européenne a émis le 29 mai 2000, dans le cadre de la lutte contre la pédophilie, une décision[105] par laquelle il demande que soit examiné le caractère obligatoire on non de la conservation par les fournisseurs d'accès Internet des données de trafic et de leur mise à disposition au bénéfice des autorités policières.

[102] Arrêt Kruslin, op.cit.

[103] Projet de convention op.cit. La Recommandation n° R(95) relative aux problèmes de procédure pénale ne prévoyait d'obligation de collaboration que pour les données conservées par les prestataires. Elle n'envisageait pas d'obligation de conservation. Sur ce point, le commentaire de la Recommandation de P. CSOUKA, Criminal procédural Law and Information Technology, 1996, CLSR, 12, p. 40.

[104] *Regulation of Investigatory Powers Bill, op.cit*., Section 30(2). Le texte prévoit un contrôle de la motivation donnée (Section 34) et la possibilité de refus contre une telle décision par la personne requise (Section 36).

[105] Décision du Conseil pour combattre la pornographie infantile sur Internet, 29 mai 2000. Cette décision fait suite à un rapport du comité des libertés et droits des citoyens adopté par le Parlement européen le 11 avril 2000 qui préconisait en outre l'obligation à charge des fournisseurs d'accès Internet de faire en sorte que l'identité des personnes qui obtiennent une adresse électronique soit vérifiée.

CONCLUSIONS

Les technologies de l'information envahissent nos vies. Leur utilisation multipliée laisse des traces. Ces traces permettent de suivre nos déplacements[106] , elles enregistrent nos messages, nos transactions, nos choix culturels, nos habitudes, ou nos déviances bien mieux et plus sûrement que les technologies classiques.

Certes, ces mêmes technologies du présent et du futur autorisent aussi, de manière plus discrète qu'auparavant, la réalisation d'infractions et ce à distance, permettant en quelques secondes de détruire ou déplacer la preuve de la réalisation de ces infractions. La presse se complaît d'ailleurs à signaler ces infractions, mettant en exergue les sites nazis, et autres sites Internet illégaux . En même temps, le monde économique s'émeut du copiage des œuvres et de l'attaque des sites commerciaux.

Ces émois conjugués justifient aux yeux de beaucoup de nos gouvernements une lutte accrue contre la cybercriminalité. Le projet n° 214 n'échappe pas à ce mouvement. Il amplifie considérablement les moyens d'investigation de l'autorité policière en charge de la répression des infractions. Il leur permet, avec la collaboration « forcée » des entreprises du secteur[107], d'accéder aux multiples « traces » que laissent nos utilisations de ces technologies, de déjouer les mesures d'anonymat et de cryptage que ces mêmes technologies avaient mises à disposition des citoyens, bref de réaliser, comme l'affirme J. BOYLE[108], bien mieux que le «Panopticon » rêvé par J. BENTHAM un « Panopticon virtuel » que d'aucuns espèrent « global », grâce à une collaboration renforcée des autorités policières au niveau mondial.

L'enjeu de la lutte contre la criminalité informatique est là. Il ne peut s'agir pour nous de jouer au « Cassandre » mais de rappeler à la suite de notre collègue J. du JARDIN, le principe de la régularité des modes de preuve et des exigences que ce principe entraîne. Que chaque mesure édictée, que chaque application concrète des mesures soit réfléchie à l'aune du principe de proportionnalité. Les dérives vers un Etat absolu doivent être évitées et l'Etat de droit doit triompher. Merci Jean de nous l'avoir rappelé courageusement dès 1985.

---

[106] Que l'on songe au mobilophone ou aux divers gadgets de type GNSS (Global Navigation Satellite System) placés dans nos véhicules qui permettent à tout moment de nous localiser. Que l'on songe à l'utilisation des navigateurs, qui permettent aux fournisseurs d'accès ou de cookies de suivre nos déplacements sur la toile du Web, de connaître les pages regardées, l'itinéraire suivi, le temps consacré à chaque site, etc.

[107] A cet égard, le récent discours de l'Attorney General Américain J. RENO, prononcé le 19 juin devant l'Information Technology Association of America (ITAP) Cybercrime Summit. Ce discours est un plaidoyer musclé pour la coopération entre les entreprises du secteur et les autorités policières dans la dénonciation et la recherche d'infractions (discours disponible à l'adresse http://uspolicy.usembassy.be/Issues/E-Commerce/reno.062300.htm). A noter sur ce point la réaction de l'association européenne des fournisseurs d'accès à Internet (EUROISPA) qui réclame au nom de la protection des données et libertés un débat public sur les limites du droit des autorités policières à contrôler les communications électroniques (Open letter Vienna 15 March 99 from EuroISPA regarding surveillance of correspondence by law enforcement authorities, disponible à http://www.euroispa.org/enfopol.htm)

[108] J. BOYLE, Foucault in Cyberspace, Surveillance Sovereignty and Hard-Wired, Censors », disponible à http : //www.wel.american.edu/pub/faculty/boyle/fouc1.html.
L'auteur démontre que la « Internet Trinity » fondée sur la liberté d'expression est actuellement remise en cause au profit d'un monde contrôlé tant par des pouvoirs privés que publics.